(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 720 328 A1

(12) **EUROPEAN PATENT APPLICATION**
published in accordance with Art. 158(3) EPC

(43) Date of publication:
03.07.1996 Bulletin 1996/27

(21) Application number: **95925129.9**

(22) Date of filing: **14.07.1995**

(51) Int. Cl.[6]: **H04L 9/28**

(86) International application number:
PCT/JP95/01410

(87) International publication number:
WO 96/02992 (01.02.1996 Gazette 1996/06)

(84) Designated Contracting States:
DE GB SE

(30) Priority: **15.07.1994 JP 164103/94**

(71) Applicant: **NTT MOBILE COMMUNICATIONS NETWORK INC.**
Minato-ku, Tokyo 105 (JP)

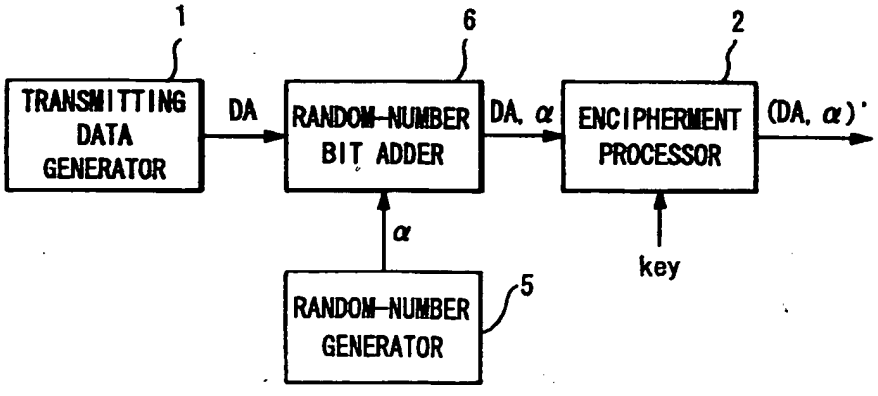
(72) Inventors:
- **MAEBARA, Akihiro**
  Yokohama-shi Kanagawa 235 (JP)
- **KOBAYASHI, Katsumi**
  Yokohama-shi Kanagawa 233 (JP)
- **OKAJIMA, Ichiro**
  Yokohama-shi Kanagawa 235 (JP)
- **UCHIDA, Noriko**
  Yokohama-shi Kanagawa 231 (JP)
- **UEBAYASHI, Shinji**
  Yokohama-shi Kanagawa 231 (JP)

(74) Representative: **KUHNEN, WACKER & PARTNER**
Alois-Steinecker-Strasse 22
85354 Freising (DE)

(54) SIGNAL TRANSMITTING METHOD AND COMMUNICATION SYSTEM

(57) Signals are transmitted in secret even when the information representing the destination terminal is opened because a common access channel is used. Obstruction can be well prevented. A random number bit adding section (6) adds a random number α (digital signal) generated by a random number generator (5) to the transmission data DA generated by a transmission data generator (1), and outputs the composite signal (DA, α). An enciphering section (2) enciphers the signal (DA, α) and outputs the ciphered signal (DA, α)'. A receiving device deciphers the ciphered signals (DA, α)' to the original signals (DA, α) and reproduces the data DA by removing the random number bit α.

FIG. 1



EP 0 720 328 A1

Description

Technical Field

This invention relates to a signal transmitting method and a communication system suited to be used for a case in which a plurality of mobile stations can access to a common access channel, for example.

Background Art

In case of a digital signal transmission in which a plurality of terminals can access to a common channel, it is necessary that identification data for identifying a transmitter's terminal and its communication counterpart are indicated. The reason is as follows. If it is unknown that a certain signal is to be transmitted from what terminal to what terminal, the signal itself becomes impossible to be transmitted because the common channel can be accessed by any terminals. The same is true to a case in which a packet communication is performed in a mobile telephone.

Incidentally, under the above-mentioned circumstance, it is customarily made open that a certain signal is to be transmitted from which terminal to which terminal. Therefore, an identification data indicative of the counterpart's terminal (or mobile station) can easily be intercepted or monitored. For this reason, an ill-willed interference can easily be performed when so desired. For example, it will be easily performed that some kind of signal is sent to the counterpart for the purpose of interference.

As a prevention measure, it can be contemplated that a signal is made secret or concealed. For the sake of convenience in the communication system, however, it is practically impossible to make secret or conceal data of the counterpart and therefore, it is only data of the transmitting signal that can be made secret.

Here, one example of a construction for enciphering a signal is depicted in Fig. 16. In Fig. 16, reference numeral 1 denotes transmitting data generator for generating data to be transmitted. Data DA prepared in the transmitting data generator 1 is enciphered by an encipherment processor 2 in accordance with a given algorithm. For encipherment, a key Key is used. For breaking the enciphered signal, the receiver side may use the same key to the one which the transmitter side uses. In that case, since the transmitter side and the receiver side are asynchronous, the receiver side cannot appropriately change the key Key but is required to use a predetermined fixed key.

In the exemplified construction in Fig. 16, the signal can be made secret if so desired. However, in case the data are simple, the original data can, in some cases, be guessed simply by seeing the enciphered result. Therefore, it cannot be said that the exemplified construction has a sufficient concealability in view of prevention of interference.

In case of control signals for mobile communication, for example, data are limited and the kind of data are also small, so small as only three in some cases. On the other hand, if the signal is enciphered using a fixed key in accordance with the same algorithm, the original signal can easily be made apparent because the kind of the enciphered signal becomes the same in number as the original signal. That is, with the method for enciphering a signal using the same key, when the kind of patterns of the signal is small, the pattern of the enciphered result becomes also small. Thus, the original signal can easily be guessed.

For the reasons mentioned above, when a signal should be monitored by an ill-willed third party who has a good knowledge of the system, there would be a large possibility that the transmitted or received signal is guessed as to what signal it is, based on data obtained from the monitored result, such as frequency of an occurrence of a certain pattern, signal length, etc., which are the results of encipherment. Especially, when the signal in question is a control signal, it can be guessed as to for what purpose the control signal is used (for example, connection, disconnection, and the like).

Once it is known for the third party that a signal is transmitted for such and such purposes, the third party can generate the same signal to the one which the genuine terminal generates, without knowing the key for concealment. As a consequence, it becomes possible for the third party to interfere the communication pretending to be the genuine terminal.

In case, for example, of a packet communication using a mobile telephone in which the kind of control signals is small, a simple encipherment is not good enough as a preventive measure of a possible interference in view of the reasons mentioned above. In addition, since a signal is transmitted in a communication circumstance easy to be monitored, an effective preventive measure against a possible interference is demanded.

Disclosure of Invention

The present invention has been developed in view of the above-mentioned situation. It is, therefore, an object of the present invention to provide a signal transmitting method and a communication system, in which a communication can fully be prevented from being interfered by a third party, by providing means of properly making secret of or concealing a transmitting signal itself even in the case where data indicative of a counterpart's terminal are obliged to be made open because of use of a common access channel.

In order to solve the above problems, the invention according to claim 1 is characterized in that the transmitter side adds a random-number bit to a predetermined position of a signal to be transmitted, enciphers the signal using a predetermined key, and then transmits the enciphered signal, and in that the receiver side breaks the encipherment of a received signal using the prede-

termined key and then removes the random-number bit from a predetermined position of the signal.

The invention according to claim 2 is characterized in that the transmitter side adds a random-number bit and an identification data for identifying a local station on the transmitter side to a predetermined position of a signal to be transmitted, enciphers the signal using a predetermined key, and then transmits the enciphered signal, and in that the receiver side breaks the encipherment of a signal received using the predetermined key, removes the random-number bit from a predetermined position of the signal whose encipherment has been broken, judges whether or not the identification data is in agreement with an identification data of a device on the transmitter side, and judges that the signal has been received in a normal condition when the first judgment result is affirmative.

The invention according to claim 3 is characterized in that a transmitting device comprises random-number generating means for generating a random-number of a predetermined bit, transmitting signal generating means for outputting a signal to be transmitted, random-number adding means for adding the random-number bit, which has been generated by the random-number generating means, to a predetermined position of the signal output by the transmitting signal generating means, and then outputting the signal, and enciphering means for enciphering an output signal of the random-number adding means, using a predetermined key, and in that a receiving device comprises encipherment-breaking means for breaking the encipherment of a received signal using the predetermined key, and random-number bit removing means for removing the random-number bit from a predetermined position of the signal output by the encipherment-breaking means and then outputting the same.

The invention according to claim 4 is characterized in that a transmitting device comprises random-number generating means for generating a random-number of a predetermined bit, transmitting signal generating means for outputting a signal to be transmitted, bit adding means for adding a random-number bit generated by the random-number generating means, and an identification data bit for identifying the transmitting device to a predetermined position of the signal output by the transmitting signal generating means, and then outputting the same, and enciphering means for enciphering the output signal of the bit adding means, using a predetermined key, and in that a receiving device comprises encipherment-breaking means for breaking the encipherment of a received signal using the predetermined key, random-number bit removing means for removing the random-number bit from a predetermined position of the output signal of the encipherment-breaking means, and judging means for judging whether or not the identification data included in the output signal of the encipherment-breaking means is in agreement with the identification data of the transmitting device, and judging that the received signal is effective when the first judgment result is affirmative.

The invention according to claim 5 is characterized in that the transmitter side generates a random-number position data indicative of a position for adding a random-number bit and adds a random-number to a bit position corresponding to the random-number position data, and in that the receiver side generates a random-number position data having the same value as the transmitter side in the same sequential order as the transmitter side, and removes the random-number from a bit position corresponding to the generated random-number position data when the random-number bit is removed.

The invention according to claim 6 is characterized in that the transmitting device comprises first random-number position data generating means for generating a random-number position data indicative of a position to which a random-number bit is to be added, the random-number adding means adding the random-number to a position corresponding to the random-number position data generated by the first random-number position data generating means, and in that the receiving device comprises second random-number position data generating means for generating a position data having the same value as the position data generated by the first random-number position data generating means in the same sequential order, the random-number bit removing means removing a random-number from a bit position corresponding to the random-number position data generated by the second random-number position data generating means.

The invention according to claim 7 is characterized in that the transmitter side generates a random-number position data indicative of a position to which a random-number bit is to be added, adds a random-number to a bit position corresponding to the random-number position data, and adds the random-number position data to the transmitting signal, and in that the receiver side extracts a random-number position data from a received signal, and removes a random-number from a bit position corresponding to the random-number position data thus extracted when the random-number is to be removed.

The invention according to claim 8 is characterized in that the transmitting device comprises random-number position data generating means for generating a random-number position data indicative of a position to which a random-number bit is to be added, and random-number position signal adding means for adding the random-number position data to the transmitting signal, the random-number adding means for adding the random-number to a position corresponding to a random-number position data generated by the random-number position data generating means, and in that the receiving device comprises random-number position data extracting means for extracting a random-number position data from the received signal, the random-number bit removing means removing a random-number from a bit position corresponding to a random-number position data extracted by the random-number position data extracting means.

The invention according to claim 9 is characterized in that said the transmitter side adds a random-number position data of a signal to be transmitted next to a signal to be transmitted immediately before, and in that the receiver side removes a random-number from a signal to be received next, based on a random-number position data extracted from a signal received immediately before.

The invention according to claim 10 is characterized in that the random-number adding means of the transmitting device adds a random-number position data of a signal to be transmitted next to a signal to be transmitted immediately before, and in that the random-number bit removing means of the receiving device removes a random-number from a signal to be received next, based on a random-number position data extracted, by the random-number position data extracting means, from a signal received immediately before.

(Operation)

Since the inventions according to claims 1 and 3 are such constructed as mentioned above, random-number bits are added to predetermined positions of a signal to be transmitted and enciphered using a predetermined key. Accordingly, the original signal cannot be restored merely by breaking the enciphered signal. On the other hand, removal of the random-number bits from predetermined positions of an encipherment-broken signal makes it possible to restore the original signal. In that case, since the signal is enciphered by being applied or added with a random-number, there can be obtained plural results of encipherment with respect to a single signal. Accordingly, the above-mentioned inconvenience can be obviated. That is, while it is very difficult for the third party to make an interference, it is easy for both the transmitter side and receiver side to make secret or conceal the data. In this case, although an address to be added to the transmitting signal is not made secret or concealed, any interference can be prevented because the third party cannot restore the enciphered signal portion to the original state even when the transmitting signal is successfully monitored by the third party.

Since the inventions according to claims 2 and 4 are such constructed as mentioned above, the transmitter side enciphers a signal to be transmitted, together with identification data combined thereto and the receiver side restores it, so that a judgment can be made as to whether identification data in the received signal is in accord with the identification data of the transmitting device. Based on the judgment result, it can be determined whether or not the received signal is a genuine one. For example, since the concealing key has a fixed length, patterns applicable to the key are limited (as one example, in case the concealing key has eight (8) bytes, the patterns applicable to the key are 2^{64}). Thus, there is a possibility that a terminal or terminals exist in which a communication is performed using the same key in the same time zone. Therefore, by applying identification data for identifying a certain terminal from others, it can be prevented that a signal from a terminal, which uses the same key, is received by mistake.

Since the inventions according to claims 5 and 6 are such constructed as mentioned above, the position where a random-number is applied can be shifted at random. Further, the receiver side can favorably restore the signal by having the same random-number adding position data as the transmitter side. Furthermore, by shifting the position of the random-number, the pattern, which occurs when the signal is enciphered, can be varied. Accordingly, a large number of patterns can be generated with small kinds of random-numbers. As a consequence, the number of patterns to be generated can extensively be increased even if the number of the random-number bits are the same as the inventions according to claims 1 and 3. This makes it very difficult for the third party to guess the content of a signal. In contrast, when the number of patterns to be generated is arranged to be the same as the inventions according to claims 1 and 3, the number of the random-number bit can be small. Thus, the same effect can be obtained with small data amount.

Since the inventions according to claims 7 and 8 are such constructed as mentioned above, the position of a random-number can be known based on the random-number position data contained in the received signal. On the other hand, in the inventions according to claims 5 and 6, the random-number adding position data are preliminarily fixedly had by both the transmitter side and receiver side and the random-number position cannot be known from the received signal. Accordingly, there is the risk that following signal cannot be received, if disagreement may occur in random-number adding position between the transmitter side and the receiver side when the signal is annihilated or the like. In contrast, in the inventions according to claims 7 and 8, by virtue of the arrangement in which the transmitting signal contains a random-number adding position data, even if a signal is annihilated, the following signal can be received in a normal condition.

Since the inventions according to claims 9 and 10 are such constructed as mentioned above, the transmitter side adds random-number position data corresponding to the next signal to the preceding signal and transmits the same, whereas the receiver side removes the random-number from a newly received signal using the random-number position data added to the preceding signal. In this way, by virtue of the arrangement in which a transmitting signal contains a random-number adding position data, there can be obtained the same effects as the inventions according to claims 7 and 8.

Brief Description of Drawings

Fig. 1 is a block diagram showing a construction of a transmitting device according to a first embodiment of the present invention.

Fig. 2 is a block diagram showing a construction of a receiving device according to the first embodiment.

Fig. 3 is a representation showing a construction of a data of an output signal in a random-number bit adder 6.

Fig. 4 is a representation showing a construction of a data of the output signal in the random-number bit adder 6.

Fig. 5 is a representation showing another construction of a data of the output signal in the random-number bit adder 6.

Fig. 6 is a block diagram showing the other construction of a transmitting device according to a modification of the first embodiment of the present invention.

Fig. 7 is a block diagram showing a construction of a receiving device according to the modification of the first embodiment.

Fig. 8 is a representation showing a construction of a data of an output signal in a bit adder 9.

Fig. 9 is a block diagram showing a construction of a transmitting device according to a second embodiment of the present invention.

Fig. 10 is a block diagram showing a construction of a receiving device according to the second embodiment.

Fig. 11A is a representation for explaining the functions of random-number position data RP.

Fig. 11B is a representation for explaining the functions of random-number position data RP.

Fig. 11C is a representation for explaining the functions of random-number position data RP.

Fig. 12 is a block diagram showing a construction example of a transmitting device according to a third embodiment of the present invention.

Fig. 13 is a block diagram showing a construction example of a receiving device according to the third embodiment.

Fig. 14 is a block diagram showing a construction of a random-number bit adder.

Fig. 15 is a block diagram showing a construction of a random-number bit remover.

Fig. 16 is a block diagram showing a general construction example in which transmitting data is enciphered.

Best Mode for Carrying Out the Invention

A-1: Construction of First Embodiment

A transmitting device in the first embodiment according to the present invention will be described with reference to Fig. 1. Reference numeral 1 shown in this illustration denotes a transmitting data generator for generating a signal to be transmitted, and reference numeral 2 denotes an encipherment processor for making an encipherment, these being the same to those shown in Fig. 16. Reference numeral 5 denotes a random-number generator for generating a random-number. A random-number α (digital signal) thus generated is added to a signal DA in a random-number bit adder 6. In this case, the random-number α is generated in a preliminarily determined bit number.

In the random-number bit adder 6, as shown in Fig. 3, bits of the random-number α are added to the signal DA and output as a signal (DA, α). Then, in the encipherment processor 2, the signal (DA, α) is enciphered and output as a signal (DA, α)'.

Fig. 2 is a block diagram showing a construction of a receiving device of this embodiment. In this illustration, reference numeral 10 denotes an encipherment-breaking processor for breaking the encipherment of the signal (DA, α)' sent thereto, using a predetermined key Key. The encipherment-breaking processor 10 outputs a signal (DA, α) as a result of encipherment. Then, a random-number bit remover 11 removes the random-number bits α from the signal (DA, α) and transmit it in the form of a signal DA alone to a circuit of a later stage.

A-2: Operation of First Embodiment

According to the above-mentioned construction, a signal output by the transmitting device is a signal obtained by enciphering the signal DA added with the random-number α. Accordingly, even in the case where the kind of the signal DA is small, the kind of the signal output by the transmitting device is remarkably increased in accordance with the bit number of the random-number.

In this case, since the enciphered signal is changed in various ways in accordance with the random-number α without any change in algorithm for encipherment and in its key Key, the signal DA cannot be guessed from (DA, α)'. Thus, concealability of signal is greatly enhanced.

On the other hand, in the receiving device, the signal (DA, α)' is encipherment-broken in the encipherment-breaking processor 10 using the fixed key Key and then, the random-number bits are removed in the random-number bit remover 11. By doing this, the signal DA can easily be reproduced.

In the above-mentioned procedure, if the algorithm for encipherment, key Key, bit number of the random-number α, and insert positions of the random-number bits are preliminarily decided between the transmitting device and the receiving device, the signal DA generated by the transmitting device can assuredly be reproduced in the receiving device.

It should be noted that although the bits of the random-number α are added to positions after the signal DA in the example shown in Fig. 3, the adding positions of the random-number are not limited to this. The random-number adding position may be a starting part of the signal DA, or it may be inserted into an intermediate part of the signal DA as shown in Fig. 4. What is essential here is that as long as the bit positions are known, the signal DA can easily be reproduced on the receiving device side.

Furthermore, the random-number bits may be divided into $\alpha 1$ and $\alpha 2$ and then added to the signal DA as shown in Fig. 5.

A-3: Modification of First Embodiment

Next, a modification of the above-mentioned embodiment will be described with reference to Figs. 6 to 8. In this modification, first, as shown in Fig. 6, identification data ID for identifying the specific device are generated in the identification data generator 8 and the identification data ID and random-number α are added to the signal DA in the bit adder 9 (see Fig. 8). As a consequence, the signal output from the encipherment processor 2 becomes (DA, ID, α).

In the receiving device, a judging unit 15 makes a following judgment with respect to the signal (DA, ID) output from the random-number bit remover 11. The judging unit 15 reads the identification data ID contained in the signal (DA, ID) and judges whether or not the identification data ID thus read are in agreement with the identification data of the transmitting device. The ID of the transmitting device is preliminarily recognized by means of a prior communication, or is preliminarily registered through a setting operation with respect to a device to be subjected to communication.

When an agreement of the identification data is detected in the judging unit 15, a judgment is made to the effect that a normal receiving is performed and the signal DA contained in the received signal is transmitted, as regular data, to a later stage. On the other hand, when an agreement of the identification data is not detected in the judging unit 15, the specific received-signal is invalidated.

In this modification, the signal is concealed using a random number and in addition, agreement of identification data between the transmitter side and the receiver side is judged. Thus, this modification is extremely effective against interference.

In case a packet communication is performed in the above modification, the identification data ID contained in the enciphered signal may be compared with data for identifying a device, which data are usually included in a part of the header of the packet. In this case, the unconcealed identification data included in the header can easily be monitored from outside. However, the identification data ID contained in the enciphered signal are not known. Accordingly, any interference attempt to transmit a signal resembling the header portion would be unsuccessful because the received signal is invalidated in the judging unit 15.

B: Second Embodiment

A second embodiment of the present invention will now be described with reference to Figs. 9 and 10. Fig. 9 depicts a construction of the transmitter side, whereas Fig. 10 depicts a construction of the receiver side. In the illustrations, like parts of the first embodiment are denoted by like reference numerals.

Reference numeral 20 of Fig. 9 denotes a memory in which a plurality of random-number position data RP indicative of random-number bits insert positions are stored. In this case, the random-number α is inserted, as shown in Figs. 11A and 11B, in the bit positions indicated by the random-number position data RP. In case the random-number is divided into $\alpha 1$ and $\alpha 2$ as in the above-mentioned modification, corresponding random-number position data are prepared (see random-number position data RP1, RP2 of Fig. 11C).

A control unit 21 of Fig. 9 adds random-number position data RP, which are read from a memory 20, to a signal DA (original data) which is output by a transmitting data generator 1 and transmits the same to a random-number bit adder 22. The random-number bit adder 22 inserts a random-number α to the signal DA in the bit position indicated by the random-number position data RP. The random-number α-added signal (DA, α) is enciphered by an encipherment processor 2 and then output as a signal (DA, α)'.

In a memory 30 shown in Fig. 10, a plurality of random-number position data RP are stored as in the case with the afore-mentioned memory 20. In this case, the stored content of the memory 20 is strictly coincident with that of the memory 30. The control unit 31 adds the random-number position data RP (or RP1, RP2) read from the memory 20 to the signal (DA, α) enciphered by the encipherment-breaking processor 10 and transmits the same to a random-number bit remover 32. At this time, the sequential order of the random-number position data read from the memory 20 is the same to the reading sequential order of the control unit 21 on the transmitter side. Therefore, the random-number position data RP read from the memory 30 are served as data indicative of the insert position of the random-number α in the received signal (DA, α). The random-number bit remover 32 removes the random-number α from the signal (DA, α) based on the content of the random-number position data RP and outputs the signal DA (original data).

As discussed above, since the random-number insert position is appropriately shifted in this embodiment, concealability of a signal is greatly enhanced.

It should be noted that although the random-number insert position is shifted based on the random-number position data RP prestored in the memory in this embodiment, it may be shifted based on time data, etc. What is essential here is that the random-number positions recognized between the transmitter side and the receiver side are synchronous.

C: Third Embodiment

Next, the third embodiment will be described with reference to Figs. 12 and 13. Corresponding parts of the illustrations to those of the respective embodiments mentioned above are denoted by identical reference numerals and description thereof is omitted.

An add position data generator 40 of Fig. 12 generates random-number position data RP indicating an adding position for a random-number α. The random-number position data RP of this case are a random value or a variable value in accordance with a predetermined

rule. Also, an initial value of the random-number position data RP is stored in the memory 41. When supplied with the signal DA (original data) from the transmitting data generator 1, the control unit 21 transmits the same to a random-number bit adder 42 and an add position data applier 43 together with the random-number position data RP read from the memory 41 and substitutes the random-number position data RP newly prepared by the add position data generator 40 in the memory 41.

As in the case with the second embodiment, the random-number bit adder 42 inserts a random-number α in a corresponding position to the random-number position data RP in the signal DA to prepare a signal (DA, α) and outputs the same. The add position data applier 43 applies the random-number position data RP to a predetermined position of the signal (DA, α) and outputs the same as a signal (DA, α, RP). This signal is enciphered by the encipherment processor 2 and transmitted to the receiver side of Fig. 13 as a signal (DA, α, RP).

An initial value of a random-number position data RP is stored in a memory 50 of Fig. 13. This value is the same to that in the memory 41. When supplied with a signal (DA, α, RP) from an encipherment-breaking processor 10, a control unit 32 transmits the same to a random-number bit remover 51 together with the random-number position data RP read from the memory 50. In the random-number bit remover 51, as in the case with the afore-mentioned embodiment, the random-number α is removed with reference to the random-number position data RP to prepare a signal (DA, RP) and the signal (DA, RP) is transmitted to an add position data remover 52. In the add position data remover 52, the random-number position data RP are discriminated from the signal (DA, RP) to restore the signal DA so as to be output. At the same time, the discriminated random-number position data RP are transmitted to the control unit 32. Also, the random-number position data RP transmitted to the control unit 32 are written for renewal in the memory 50.

As described above, the random-number position data RP corresponding to the next signal are added to the preceding signal and transmitted on the transmitter side, whereas the random-number α is removed from a newly received signal using the random-number position data RP added to the preceding signal on the receiver side. Accordingly, the random-number position data RP used on the transmitter side are always coincident with the random-number position data RP used on the receiver side.

In the above description, the random-number position data RP of the next transmitting signal are added to the preceding transmitting signal. In the alternative, the random-number position data RP used for the current transmitting signal may be added directly to the current transmitting signal. It should be noted, however, that concealability of signal is higher in the case of the above-mentioned embodiment.

D: Others

(1) Re: Random-Number

As the random-number in the above-mentioned respective embodiments, those generated by a known random-number generator may be used. It is also acceptable that a random-number table is stored in a memory and a random-number is generated by appropriately reading this random table.

Also, a numeric value, which cannot be defined as a random-numbers in a strict sense, may be used. For example, time information output by a timer and output values of a counter for sequentially counting a given clock may be used.

(2) Re: Encipherment

Various algorithms may be used for encipherment. The encipherment is classified roughly into two: secret key method and open key method. This classification is made based on the way of use of an encipherment key. Any of the two may be applied to the present invention.

In the case of the secret key method, it is required for both the transmitter side and the receiver side to preliminarily have the same key. This method enables a high-speed operation and is, therefore, practical. The key in this secret key method may be preliminarily fixedly stored on both the transmitter side and the receiver side or the key may be delivered at the start of a communication.

As a known encipherment algorithm for the secret key method, there is an FEAL (Fast Data Encipherment Algorithm). This algorithm is discussed in detail, for example, on pages 43 to 49 of "Encipherment and Data Security" (co-written by Shigeo Tsujii and Masao Kasahara: issued by Shokodo).

(3) Example of Construction of Random-Number Bit Adder

One example of a construction of the random-number bit adders 6, 22 and 42 of the above-mentioned respective embodiments is depicted in Fig. 14. In a circuit depicted in this illustration, a signal DA and a random-number α are transmitted to shift registers 60 and 61, respectively. Based on clock CK supplied from a clock generator 62 respectively through AND getes 63 and 64, the shift registers 60 and 61 shift the signal DA and the random-number α by a bit each time and output the same. A counter 66 is adapted to cyclically count the clock CK and the counting cycle corresponds to a combined length of the signal DA and random-number α (or α1, α 2). A decoder 67 is adapted to decode the value counted by the counter 66. The decoder 67 outputs a signal "1" from a count value corresponding to the random-number position data RP (or RP1, RP2) to a count value corresponding to the random-number α (or α1, α 2) and outputs a signal "0" in other count values. The

output signals of the decoder 67 are supplied to the AND gate 64 and also to the AND gate 63 through an inverter 65.

According to the above-mentioned construction, the output signal of the decoder 67 is "0" in all other positions than the bit position of the random-number α designated by the random-number position data RP. As a consequence, the AND gate 63 is brought to be open, the AND gate 64 is brought to be closed, and the shift register 60 alone performs the shifting operation. Consequently, the signal DA in the shift register 60 is output through an OR gate 68. On the other hand, the output signal of the decoder 67 is "1" in the bit position of the random-number α (or α1, α2) designated by the random-number position data RP (or RP1, RP2). As a consequence, the AND gate 63 is brought to be closed, the AND gete64 is brought to be open, and the shift register 61 alone performs the shifting operation. Consequently, the random-number α (or α1, α2) is output from the OR gate 68. In this way, a signal having the random-number α applied to a predetermined position of the signal DA is prepared.

The afore-mentioned bit adder 9 adds not only the random-number α but also the identification data ID. The adding portion of the random-number α can be realized with the above-mentioned circuit construction.

It should be noted that the above-mentioned circuit example is only one example and other circuit constructions may be employed. Also, the same purpose may be realized by means of software processing.

(4) constitutional Example of Random-Number Bit Remover

Fig. 15 is a block diagram showing one example of a construction of the random-number bit remover 11, 22, 32, 51.

In the circuit depicted in the illustration, data of a combination of the signal DA and random-number α are transmitted to a shift register 70. A clock signal CK output from a clock generator 71 is transmitted to the shift register 70, a counter 72, and an AND gate 75. The counter 72 is adapted to cyclically count the clock CK and the count cycle corresponds to the combined length of the signal DA and the random-number α (or α1, α2). The decoder 73 is adapted to decode the count value of the counter 72. The decoder 73 outputs a signal "0" from the count value corresponding to the random-number position data RP (or RP1, RP2) to the random-number α (or α1, α2) and outputs a signal "1" in other count values. The output signals of the decoder 73 are supplied to the AND gates 74 and 75.

According to the above-mentioned construction, signals (DA, α) are output, one after another, from the shift register 70 in synchronism with the clock signal CK. Since the output signal of the decoder 73 is "1" in other position than the bit position of the random-number α designated by the random-number position data RP, the AND gate 75 is brought to be open and the shift register 76 performs the shifting operation. Since the AND gate 74 is also open at this time, the data output, one after another, from the shift register 70 are transmitted, one after another, to the shift register 76 through the AND gate 74.

On the other hand, the output signal of the decoder 73 is "0" in the bit position of the random-number α designated by the random-number position data RP. As a consequence, the AND gates 74 and 75 are brought to be closed and the shift register 70 alone performs the shifting operation. Consequently, the random-number α (or α1, α2) output from the shift register 70 does not pass through the AND gate 74 and is discarded. Since the shift register 76 does not perform the shifting operation at this time, no input side empty bit is generated. When other bit positions than the random-number α come, the AND gates 74 and 75 are brought to be open again and the shift register 76 starts the shifting operation. As a consequence, the signal DA is transmitted to the shift register 76. By means of the afore-mentioned operation, only the signal DA is extracted in the shift register 76.

It should be noted that the above-mentioned circuit example is only one example and other circuit constructions may be employed. Also, the same purpose may be realized by means of software processing.

E: Effect

As described in the foregoing, in the above-mentioned respective embodiments, a signal is added with a random-number and then enciphered. Accordingly, encipherment of a single signal results in generation of a plurality of designs. By this, for example, even in the case where data are obliged to be open because a common access channel is used, the transmitting signal itself can favorably be concealed and interference can fully be prevented from occurrence.

Industrial Applicability

This invention is suited to be used for a case in which a plurality of mobile stations can access to a common access channel, for example. The invention can also be used for communication in which concealment is necessary. It can also be applied to a case in which a packet communication is performed in a mobile communication.

Claims

1. A signal transmitting method characterized in that
   the transmitter side:
   adds random-number bits to predetermined positions of a signal to be transmitted, enciphers the signal using a predetermined key, and then transmits the enciphered signal, and in that
   the receiver side:
   breaks the encipherment of a received signal using said predetermined key and then removes said random-number bit from predetermined positions of said signal.

2. A signal transmitting method characterized in that
the transmitter side
adds random-number bits and identification data for identifying a local station on said the transmitter side to predetermined positions of a signal to be transmitted, enciphers the signal using a predetermined key, and then transmits the enciphered signal, and in that
the receiver side
breaks the encipherment of a signal received using said predetermined key, removes said random-number bits from predetermined positions of the signal whose encipherment has been broken, judges whether or not said identification data are in agreement with identification data of a device on the transmitter side, and judges that the signal has been received in a normal condition when the first judgment result is affirmative.

3. A communication system characterized in that
a transmitting device comprises:
random-number generating means for generating a random-number of predetermined bits;
transmitting signal generating means for outputting a signal to be transmitted;
random-number adding means for adding said random-number bits, which has been generated by said random-number generating means, to predetermined positions of the signal output by said transmitting signal generating means, and then outputting the signal; and
enciphering means for enciphering an output signal of said random-number adding means, using a predetermined key; and in that
a receiving device comprises:
encipherment-breaking means for breaking the encipherment of a received signal using said predetermined key; and
random-number bit removing means for removing said random-number bits from predetermined positions of the signal output by said encipherment-breaking means and then outputting the same.

4. A communication system characterized in that
a transmitting device comprises:
random-number generating means for generating a random-number of predetermined bits;
transmitting signal generating means for outputting a signal to be transmitted;
bit adding means for adding random-number bits generated by said random-number generating means, and identification data bits for identifying said transmitting device to predetermined positions of the signal output by said transmitting signal generating means, and then outputting the same; and
enciphering means for enciphering the output signal of said bit adding means, using a predetermined key; and in that
a receiving device comprises:
encipherment-breaking means for breaking the encipherment of a received signal using said predetermined key;
random-number bit removing means for removing said random-number bits from predetermined positions of the output signal of said encipherment-breaking means; and
judging means for judging whether or not said identification data included in the output signal of said encipherment-breaking means are in agreement with said identification data of said transmitting device, and judging that the received signal is effective when the first judgment result is affirmative.

5. A signal transmitting method according to claim 1 or 2, characterized in that
said the transmitter side generates a random-number position data indicative of a position for adding random-number bits and adds a random-number to bit positions corresponding to said random-number position data, and in that
said the receiver side generates a random-number position data having the same value as said the transmitter side in the same sequential order as said the transmitter side, and removes the random-number from bit positions corresponding to the generated random-number position data when said random-number bits are removed.

6. A communication system according to claim 3 or 4, characterized in that
said transmitting device comprises:
first random-number position data generating means for generating random-number position data indicative of positions to which random-number bits are to be added, said random-number adding means adding said random-number bits to positions corresponding to the random-number position data generated by said first random-number position data generating means; and in that
said receiving device comprises:
second random-number position data generating means for generating position data having the same value as the position data generated by said first random-number position data generating means in the same sequential order, said random-number bit removing means removing random-number bits from bit positions corresponding to said random-number position data generated by said second random-number position data generating means.

7. A signal transmitting method according to claim 1 or 2, characterized in that
said the transmitter side generates random-number position data indicative of positions to which random-number bits are to be added, adds random-number bits to bit positions corresponding to said

random-number position data, and adds said random-number position data to said transmitting signal; and in that

said the receiver side extracts random-number position data from a received signal, and removes random-number bits from bit positions corresponding to the random-number position data thus extracted when the random-number bits are to be removed.

8. A communication system according to claim 3 or 4, characterized in that

said transmitting device comprises random-number position data generating means for generating random-number position data indicative of positions to which random-number bits are to be added, and random-number position signal adding means for adding said random-number position data to said transmitting signal, said random-number adding means for adding said random-number bits to positions corresponding to random-number position data generated by said random-number position data generating means; and in that

said receiving device comprises random-number position data extracting means for extracting random-number position data from the received signal, said random-number bit removing means removing random-number bits from bit positions corresponding to random-number position data extracted by said random-number position data extracting means.

9. A signal transmitting method according to claim 7, characterized in that said the transmitter side adds a random-number position data of a signal to be transmitted next to a signal to be transmitted immediately before, and in that said the receiver side removes random-number bits from a signal to be received next, based on a random-number position data extracted from a signal received immediately before.

10. A communication system according to claim 8, characterized in that

said random-number adding means of said transmitting device adds random-number position data of a signal to be transmitted next to a signal to be transmitted immediately before; and in that

said random-number bit removing means of said receiving device removes random-number bits from a signal to be received next, based on random-number position data extracted, by said random-number position data extracting means, from a signal received immediately before.

FIG. 1

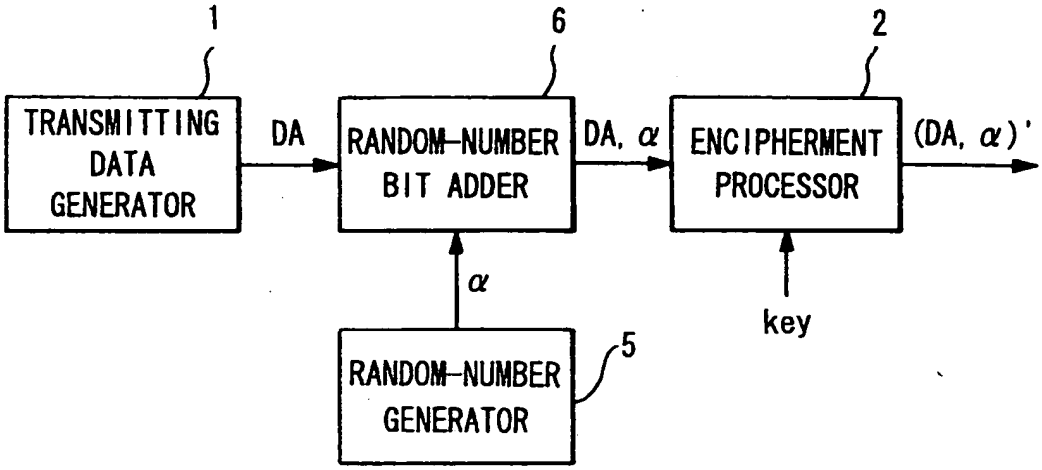


FIG. 2

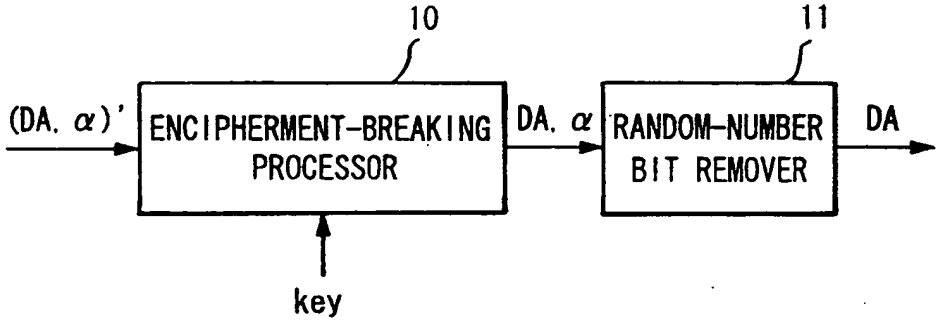


FIG. 3

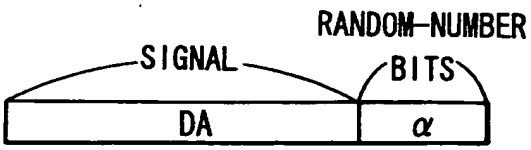


FIG. 4

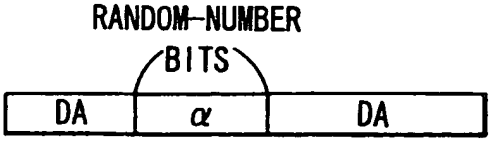


FIG. 5

FIG. 6

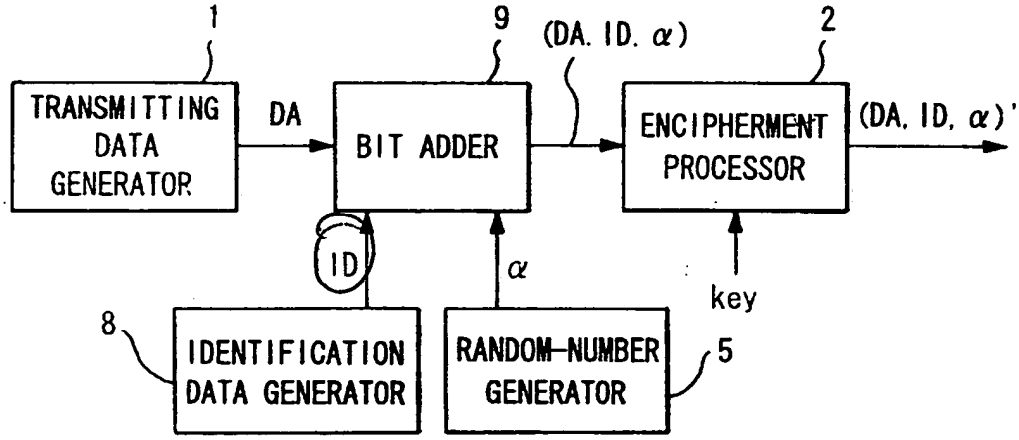


FIG. 7

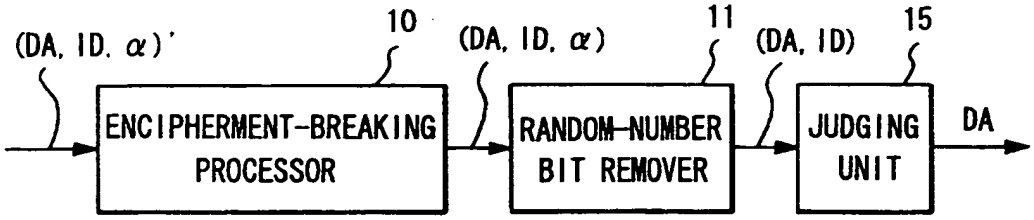


FIG. 8

FIG. 9

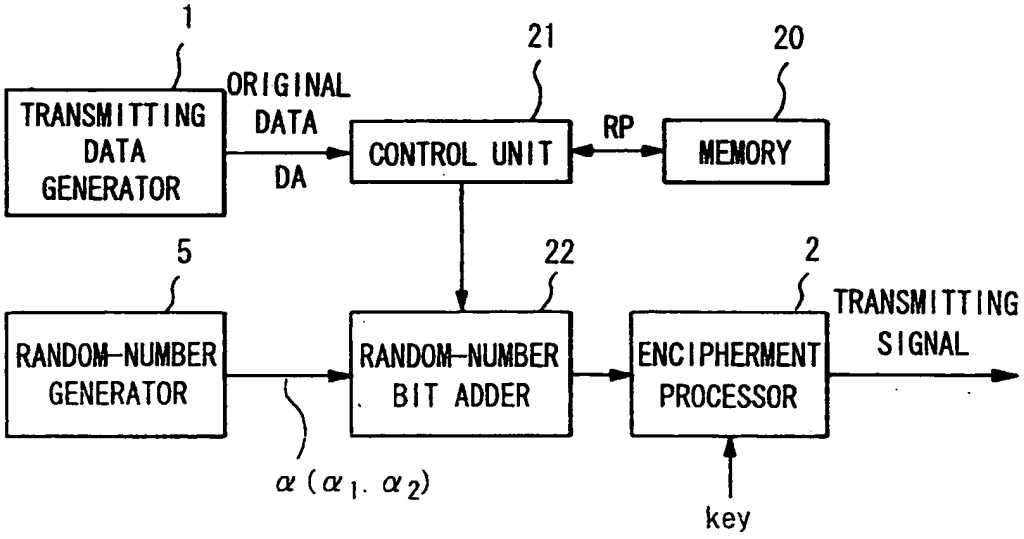

1
TRANSMITTING DATA GENERATOR
ORIGINAL DATA
DA
21
CONTROL UNIT
RP
20
MEMORY
5
RANDOM-NUMBER GENERATOR
22
RANDOM-NUMBER BIT ADDER
2
ENCIPHERMENT PROCESSOR
TRANSMITTING SIGNAL
α (α1, α2)
key

FIG. 10

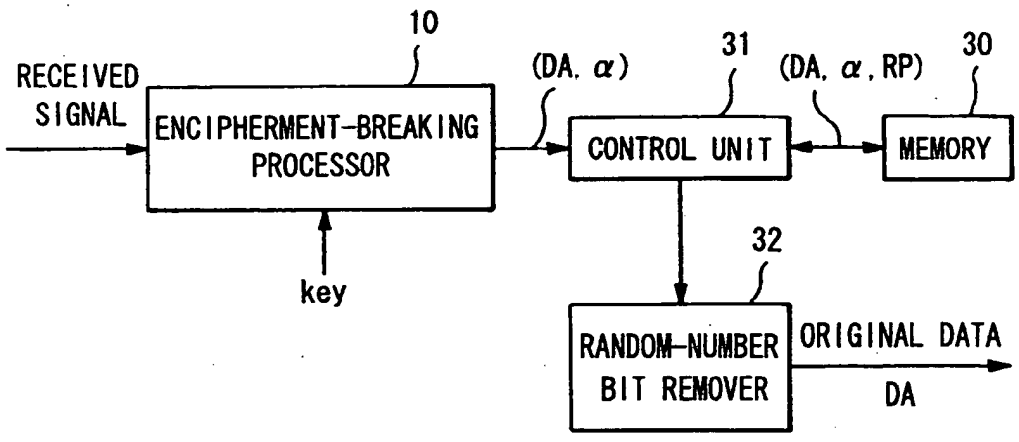

RECEIVED SIGNAL
10
ENCIPHERMENT-BREAKING PROCESSOR
key
(DA, α)
31
CONTROL UNIT
(DA, α, RP)
30
MEMORY
32
RANDOM-NUMBER BIT REMOVER
ORIGINAL DATA
DA

FIG. 11A

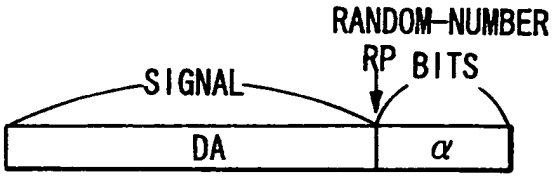


FIG. 11B

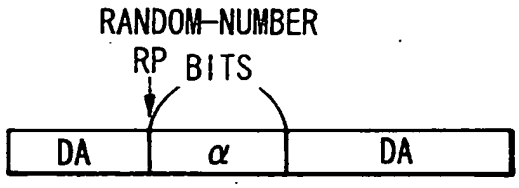


FIG. 11C

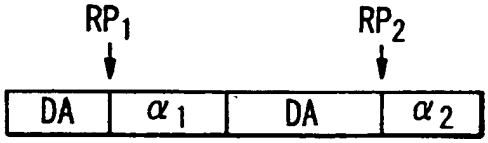


FIG. 12

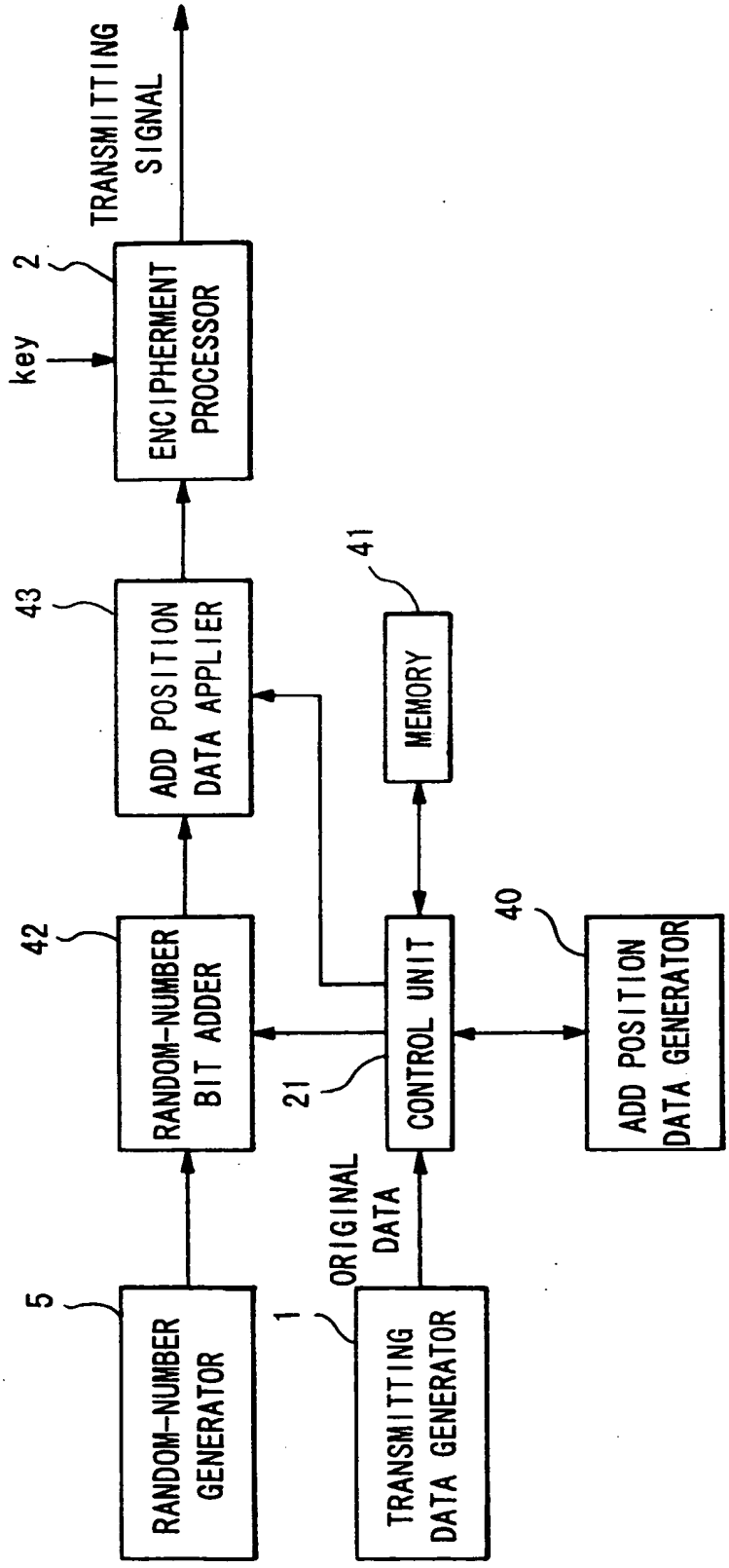

TRANSMITTING SIGNAL
2
key
ENCIPHERMENT PROCESSOR
43
ADD POSITION DATA APPLIER
41
MEMORY
42
RANDOM-NUMBER BIT ADDER
21
CONTROL UNIT
40
ADD POSITION DATA GENERATOR
5
RANDOM-NUMBER GENERATOR
1
ORIGINAL DATA
TRANSMITTING DATA GENERATOR

FIG. 13

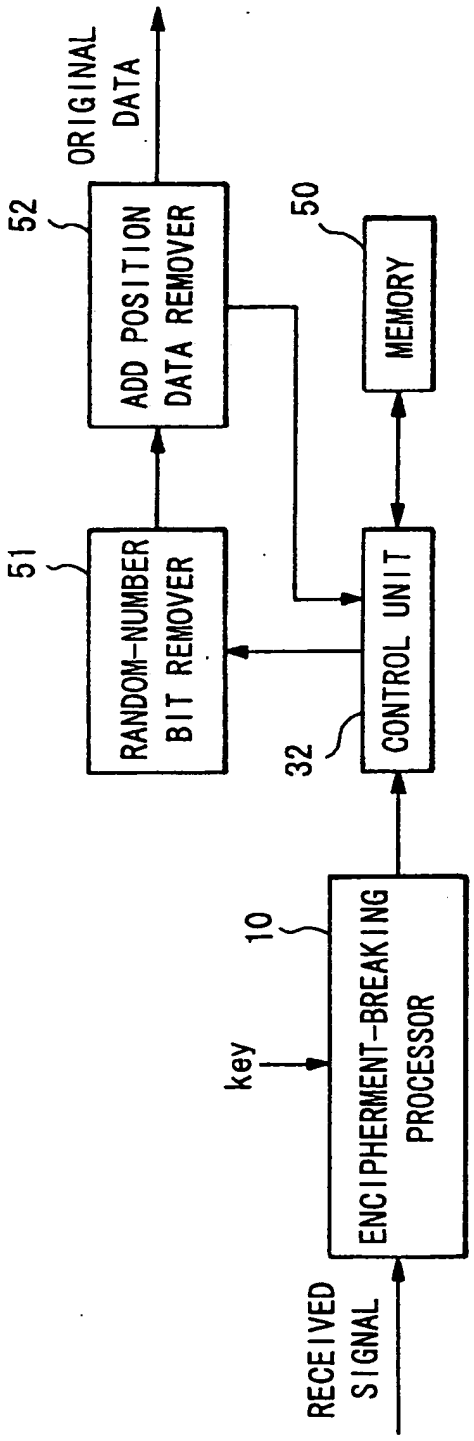

RECEIVED SIGNAL
ENCIPHERMENT-BREAKING PROCESSOR
10
key
CONTROL UNIT
32
MEMORY
50
RANDOM-NUMBER BIT REMOVER
51
ADD POSITION DATA REMOVER
52
ORIGINAL DATA

FIG. 14

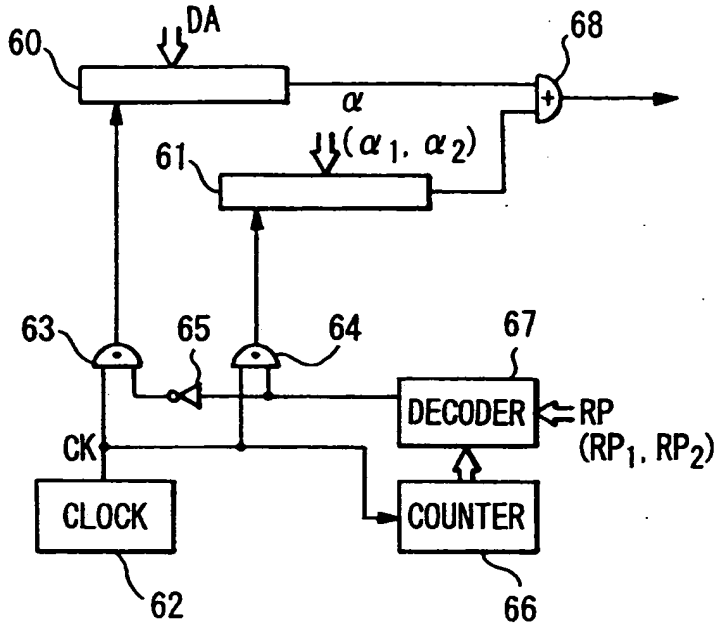

60
DA
68
α
61
(α1, α2)
63
65
64
67
DECODER
RP
(RP1, RP2)
CK
CLOCK
COUNTER
62
66

FIG. 15

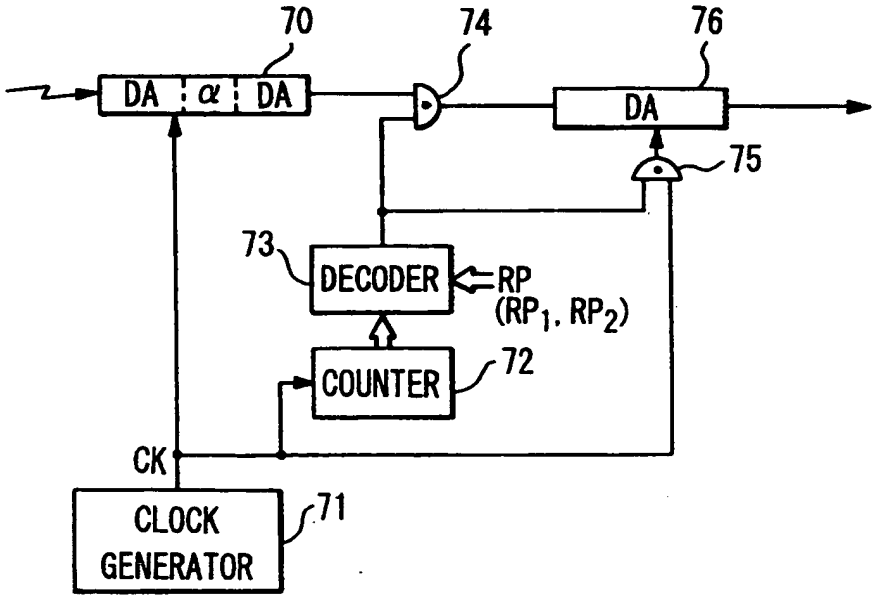
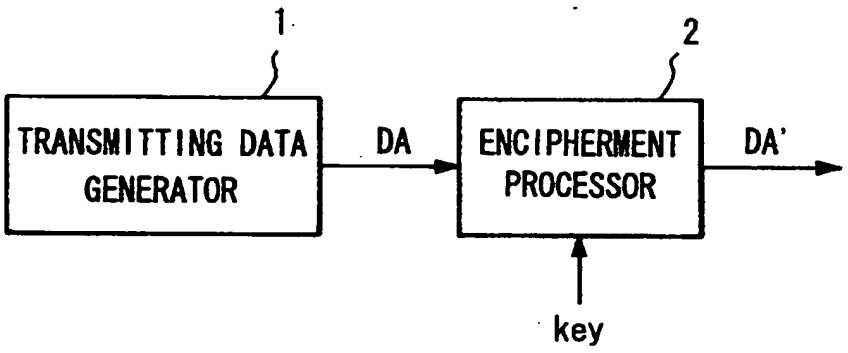

70
74
76
DA
α
DA
DA
75
73
DECODER
RP
(RP1, RP2)
COUNTER
72
CK
CLOCK
GENERATOR
71

FIG. 16


1
2
TRANSMITTING DATA GENERATOR
DA
ENCIPHERMENT PROCESSOR
DA'
key

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP95/01410

A. CLASSIFICATION OF SUBJECT MATTER
Int. Cl^6 H04L9/28

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int. Cl^6 H04L9/00, H04K1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926 - 1995
Kokai Jitsuyo Shinan Koho 1971 - 1995

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 4-101529, A (Nittsuko K.K.), April 3, 1992 (03. 04. 92), Line 5, lower left column to line 10, lower right column, page 2, line 16, upper left column to line 1, upper right column, page 3 (Family: none)	1 - 10
Y	JP, 1-194627, A (NEC Corp.), August 4, 1989 (04. 08. 89), Line 8, lower right column, page 1 to line 13, upper left column, page 2 (Family: none)	1 - 10
Y	JP, 63-248240, A (Canon Inc.), October 14, 1988 (14. 10. 88), Line 2, upper left column to line 8, upper right column, page 2, lines 12 to 16, lower right column, page 2 (Family: none)	1 - 10
Y	JP, 1-284037, A (NEC Corp.), November 15, 1989 (15. 11. 89), Line 2, upper left column, page 2 to line 8,	9 - 10

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
September 21, 1995 (21. 09. 95)	October 9, 1995 (09. 10. 95)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP95/01410

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	upper left column, page 3 (Family: none)	
Y	JP, 1-212039, A (Toshiba Corp.), February 14, 1989 (14. 02. 89), Claim (Family: none)	2, 4-10

Form PCT/ISA/210 (continuation of second sheet) (July 1992)